

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

05/31/2016

SUBJECT:

Vulnerability in DotNetNuke (DNN) Content Management System Could Allow for Unauthorized Access

OVERVIEW:

A vulnerability has been discovered in DotNetNuke, which could allow for unauthorized access. DNN is a content management system (CMS) for websites. Successful exploitation could result in an attacker gaining Super User access to the CMS allowing access to sensitive information, and the ability to add, remove, or modify content. An attacker can also utilize the vulnerability in phishing campaigns to redirect unsuspecting users to a malicious site.

THREAT INTELLIGENCE:

This vulnerability has been observed being exploited in the wild.

SYSTEM AFFECTED:

- DNN versions prior to 8.0.3

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:

Due to a failure to remove files required for installation of DNN a remote attacker is able to leverage a specially crafted URL to access the install wizard and create Super User accounts. Specifically this occurs when the files InstallWizard.aspx and InstallWizard.aspx.cs exist under the Website Root\Install folder. DNN has released version 8.0.3 to address this issue.

Successful exploitation could result in an attacker gaining Super User access to the CMS allowing access to sensitive information, and the ability to add, remove, or modify content.

DNN has also released a work around which entails manually removing the following files from the Website Folder\Install location.

- DotNetNuke.install.config
- DotNetNuke.install.config.resources
- InstallWizard.aspx
- InstallWizard.aspx.cs
- InstallWizard.aspx.designer.cs
- UpgradeWizard.aspx
- UpgradeWizard.aspx.cs
- UpgradeWizard.aspx.designer.cs
- Install.aspx
- Install.aspx.cs
- Install.aspx.designer.cs

RECOMMENDATIONS:

The following actions should be taken:

- Update DNN CMS to the latest version after appropriate testing.
- Verify that all files listed above have been removed, and review current Super User accounts for unauthorized access.
- Verify that no unauthorized changes have occurred on the system prior to implementing patches.
- Confirm that the operating system and all other applications on the system running this CMS are updated with the most recent patches.

REFERENCES:

DNN:

<http://www.dnnsoftware.com/platform/manage/security-center>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>